**IN THE UNITED STATES DISTRICT COURT**
**FOR THE DISTRICT OF MARYLAND,**
**GREENBELT DIVISION**

| | |
|---|---|
| MARC WEINBERG and VICTORIA NEIKIRK,<br><br>Plaintiffs,<br>v.<br><br>MARRIOTT INTERNATIONAL INC. and STARWOOD HOTELS & RESORTS WORLDWIDE, LLC,<br><br>Defendants. | Case No.<br><br>CLASS ACTION COMPLAINT<br><br>JURY TRIAL DEMANDED |

Plaintiffs Marc Weinberg and Victoria Neikirk (ñPlaintiffsò), by and through their undersigned counsel, submit this Complaint on behalf of themselves and all others similarly situated. Plaintiffsô allegations are based upon their personal knowledge as to themselves and their own acts, and upon information and belief, developed from the investigation and analysis by Plaintiffsô counsel, including a review of publicly available information.

## NATURE OF THE ACTION

1. Plaintiffs bring this class action case against Marriott International, Inc. (ñMarriottò) and Starwood Hotels & Resorts Worldwide, LLC (ñStarwoodò) (the ñDefendantsò or collectively the ñCompanyò) for their failure to secure and safeguard the personally identifiable information (ñPIIò) of up to approximately 500 million of their customers, including passport numbers of up to 327 million of these customers[1] which Marriottôs Starwood division

[1] See article entitled ñBiggest Prize in Marriott hack: Passport numbersò in ñPOLITICO/CYBERSECURITYò dated 12/03/18 available online at https://www.politico.com/story/2018/12/03/biggest-prize-in-the-marriott-hack-passport-numbers-1003253

collected and maintained. The Defendants maintain and operate a customer reservation and rewards database which they refer to as the ñStarwood guest reservation database.ò This is separate from the guest reservation system Marriott uses for guest reservations for itsô non-Starwood properties. Starwood used the ñStarwood guest reservation databaseò as itsô guest reservation system before Starwood was acquired by Marriott in 2016, as more fully discussed below.

2. On November 30, 2018, Marriott disclosed that it had suffered an extremely significant data breach. It stated that ñ[o]n September 8, 2018, [it] [ ] received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States.ò Marriott learned during the investigation ñthat there had been unauthorized access to the Starwood network since 2014. The Company recently discovered that an unauthorized party had copied and encrypted PII. On November 19, 2018, Marriott was able to decrypt the PII and determined that the contents were from the Starwood guest reservation database.ò

3. The Company, in its announcement of November 30, stated that it believed the corrupted data base had information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the PII includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (ñSPGò) account information, date of birth, gender, arrival and departure information, reservation date,

4. The PII of the Plaintiffs and the other customers who used Starwoodôs reservation system they seek to represent was compromised due to Marriott and/or Starwoodôs acts and omissions and their failure to properly protect their customerôs PII.

5. Marriott and/or Starwood could have prevented this Data Breach.

6. Marriott and/or Starwood disregarded the rights of Plaintiffs and the other Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure that the Starwood data systems were protected, failing to disclose to their customers the material fact that Starwood and/or Marriott did not have adequate security practices to safeguard the PII that Starwood customers had disclosed to Starwood and/or Marriott with the understanding they would be secure; failing to take available steps to prevent and stop the breach from ever happening; and failing to monitor and detect the breach on a timely basis.

7. As a result of the Data Breach, Plaintiffs and the other Class members have been exposed, in all likelihood, to criminals for misuse of their PII. The injuries suffered by Plaintiffs and the other Class members, or likely to be suffered as a direct result of the Data Breach, include:

a. unauthorized use of their PII;

b. theft of their PII;

c. costs associated with the detection and prevention of identity theft and unauthorized use of their financial accounts;

d. damages arising from the inability to use their PII;

e. loss of use of their passports and the special difficulty in replacing passport information which is magnitudes more valuable on the digital black markets than stolen credit card information;

f. loss of use of and access to their account funds and costs associated with inability to obtain money from their accounts or being limited in the amount of money they were permitted to obtain from their accounts, including missed payments on bills

and loans, late charges and fees, and adverse effects on their credit including decreased credit scores and adverse credit notations;

g. costs associated with time spent and the loss of productivity or the enjoyment of oneôs life from taking time to address and attempt to ameliorate, mitigate and deal with the actual and future consequences of the Data Breach, including finding fraudulent charges, the costs of purchasing credit monitoring and identity theft protection services, and the stress, nuisance and annoyance of dealing with all issues resulting from the Data Breach;

h. the imminent and certainly impending injury flowing from potential fraud and identify theft posed by their PII being placed in the hands of criminals and already misused via the sale of Plaintiffsô and the other Class membersô PII on the Internet black market;

i. damages to and diminution in value of their PII entrusted to Marriott for the sole purpose of purchasing products and services from Marriott; and

j. the loss of Plaintiffsô and the other Class membersô privacy.

8. The injuries to Plaintiffs and other Class members were directly and proximately caused by Defendantsô failure to implement or maintain adequate data security measures for PII.

9. Further, Plaintiffs retain a significant interest in ensuring that their PII, which, while stolen, remains in the possession of Defendants, is protected from further breaches, and seeks to remedy the harms they have suffered on behalf of themselves and similarly situated class members whose PII was stolen as a result of the Data Breach.

10. Plaintiffs bring this action to remedy these harms on behalf of themselves and all similarly situated individuals whose PII was accessed during the Data Breach. Plaintiffs seek the

following remedies, among others: statutory damages under state and/or federal laws, reimbursement of out-of-pocket losses, payments for new passports to make it harder for thieves to paint a full identity pictureò;[2] other compensatory damages, further and more robust credit monitoring services with accompanying identity theft insurance, and injunctive relief including an order requiring Defendants to implement improved data security measures.

**PARTIES**

11. Plaintiffs Marc Weinberg is a New Jersey citizen and resident and was a user of Starwoodôs reservation system in New Jersey during the relevant time period to which he provided it his PII.

12. Plaintiffs Victoria Neikirk is a Florida citizen and resident and was a user of Starwoodôs reservation system in Florida during the relevant time period to which she provided it her PII

13. Defendant Marriott is a Delaware Corporation with its headquarters located in Bethesda, Maryland and operations virtually all around the world including in this District.

14. Defendant Starwood is a Maryland limited liability corporation with its principal place of business in Bethesda, Maryland.

15. Defendant Marriott encompasses a portfolio of more than 6,700 properties in 30 leading hotel brands spanning 129 countries and territories. Marriott operates and franchises hotels and licenses vacation ownership resorts all around the world including through the Marriottôs wholly owned subsidiary Starwood, whose data base was hacked, is the subject of this action.

[2] See article ñSchumer: Marriott should lay for new passports compromised by data breachò, *The Washington Post*, 12/03/18. Available online at https://www.washingtonpost.com/business/2018/12/03/schumer-marriott-should-pay-new-passports-compromised-by-data-breach/?noredirect=on&utm_term=.0f9df7f1a7e9

16. Defendant Starwood, prior to its acquisition as a wholly owned subsidiary of Marriott, was one of the world's largest hotel companies that owned, operated, franchised and managed hotels, resorts, spas, residences, and vacation ownership properties under its 11 owned brands. As of 1 December 2014, Starwood Hotels and Resorts had owned, managed, or franchised over 1,200 properties employing over 180,400 people. It brands included Sheraton, Four Points, Westin, W and St. Regis.

## JURISDICTION AND VENUE

17. This Court has jurisdiction over this action pursuant to the Class Action Fairness Act, 28 U.S.C. §1332(d)(2), because the amount in controversy exceeds $5,000,000, exclusive of interest and costs, and Plaintiffs is a citizen of a different state than Defendants. The proposed Class includes well over 100 members.

18. This Court has jurisdiction over Defendants because they regularly conduct business in this District and have sufficient minimum contacts in this District. Defendants intentionally availed themselves of this jurisdiction by marketing and offering their services from this District to millions of consumers nationwide, including those in the states of New Jersey and Maryland.

19. Venue is proper in this District pursuant to 28 U.S.C. §1391 because Marriott and Starwood are headquartered in this District and conduct business in this District.

## CLASS ACTION ALLEGATIONS

20. Plaintiffs bring this class action pursuant to the Federal Rules of Civil Procedure 23(a) and (b)(3), on behalf of themselves and all others similarly situated in the United States, who were users of Starwoodôs reservation system during the relevant time period and were damaged thereby (the ñClassò). Plaintiffs also bring Counts on behalf of sub-classes of users of

the Starwood reservation system who reside in New Jersey during the time the Data Breach was occurring and had their PII stolen from Marriottôs software application systems and were damaged thereby (the ñSubclassò). The Class and the Subclass exclude Marriott and Starwood officers or directors.

21. The Class and Subclass consist of potentially millions of Marriott customers who made reservations through the Starwood reservation system. While the exact number of members of the Class and Subclass and the identities of individual members of the Class and Subclass are unknown to Plaintiffsô counsel at this time, and can only be ascertained through appropriate discovery, based on the fact that up to around 500 million of Marriottôs Starwood customers have been adversely affected, the membership of the Class and Subclass are each so numerous that joinder of all members is impracticable.

22. The Defendantsô wrongful conduct affected all members of the Class and Subclass in exactly the same way. The Defendantsô failure to properly safeguard its customersô PII is completely uniform among the Class and Subclass members.

23. Questions of law and fact common to all members of the Class and Subclass predominate over any questions affecting only individual members. Such common questions of law and fact include:

a. whether the Defendants acted wrongfully by failing to properly customers PII collected and stored by Marriott or Starwood on the Starwood software application system;

b. whether Defendantsô conduct violated law;

c. whether the Plaintiffs and the other members of the Class and Subclass have been damaged, and, if so, what is the appropriate relief; and

d. whether Defendants breached their duties owed to members of the Class and Subclass and by failing to properly safeguard their PII.

24. Plaintiffsô claims, as described herein, are typical of the claims of all other members of the Class and Subclass, as the claims of Plaintiffs and all other members of the Class and Subclass arise from the same set of facts regarding Defendantsô failure to protect the Class and Subclass memberôs personal information from computer hackers. Plaintiffs maintain no interest antagonistic to the interests of other members of the Class or Subclass.

25. Plaintiffs are committed to the vigorous prosecution of this action and have retained competent counsel experienced in the prosecution of class actions of this type. Accordingly, Plaintiffs are adequate representatives of the Class and Subclass and will fairly and adequately protect their interests.

26. This class action is a fair and efficient method of adjudicating the claims of Plaintiffs and the Class and Subclass for the following reasons:

a. common questions of law and fact predominate over any question affecting any individual Class and Subclass members;

b. the prosecution of separate actions by individual Class and Subclass members would likely create a risk of inconsistent or varying adjudications with respect to individual members thereby establishing incompatible standards of conduct for Defendants or would allow some Class and Subclass membersô claims to adversely affect the ability of other members to protect their interests;

c. this forum is appropriate for litigation of this action since a substantial portion of the transactions, acts, events, and omissions alleged herein occurred in this District;

d. Plaintiffs anticipate no difficulty in the management of this litigation as a class action; and

e. the Class and Subclass are readily definable, and prosecution as a class action will eliminate the possibility of repetitious litigation, while also providing redress for claims that may be too small to support the expense of individual, complex litigation.

27. For these reasons, a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

**SUBSTANTIVE ALLEGATIONS**

28. On November 16, 2015, Marriott announced that its board and the board of Starwood approved a definitive merger agreement under which the companies would create the worldôs largest hotel company. On September 23, 2016, Marriott completed its acquisition of Starwood Hotels & Resorts.

29. Plaintiffs were customers of Starwood and who had previously made reservations to stay at one or more of the following properties in or on the Starwood reservation database: the St. Regis, Westin, Sheraton and W, Element, and Aloft Hotels, The Luxury Collection, Tribute Portfolio, Le Meridien Hotels and Resorts, Four Points by Sheraton, and Design Hotels, as well as Starwood branded timeshare properties.

30. On November 30, 2018, Marriott disclosed that it had suffered an extremely significant data breach. It stated that ñ[o]n September 8, 2018, [it] [ ] received an alert from an internal security tool regarding an attempt to access the Starwood guest reservation database in the United States.ò Marriott learned during the investigation ñthat there had been unauthorized access to the Starwood network since 2014. The Company recently discovered that an

unauthorized party had copied and encrypted PII. On November 19, 2018, Marriott was able to decrypt the PII and determined that the contents were from the Starwood guest reservation database.ò [3]

31. The Company believes the corrupted data base ñcontains information on up to approximately 500 million guests who made a reservation at a Starwood property. For approximately 327 million of these guests, the PII includes some combination of name, mailing address, phone number, email address, passport number, Starwood Preferred Guest (ñSPGò) account information, date of birth, gender, arrival and departure information, reservation date, and communication preferences. For some, the information also includes payment card numbers and payment card expiration dates, but the payment card numbers were encrypted using Advanced Encryption Standard encryption (AES-128).ò [4]

32. Marriott said hackers had gained unauthorized access to the Starwood reservation system since 2014. The Company identified and learned of the issue on September 8, 2018. Yet, Marriott did not disclose the breach to its customers until November 30, 2018. Such delay was unwarranted and directly increases the likelihood that thieves have already stolen or will be able to steal victimsô identities before victims even know that they are at risk.

33. In addition, as of November 30, 2018, Marriott had failed in its legal obligation to notify the Attorney General (the ñNYAGò) upon discovery of the breach. The NYAG has opened an investigation into the matter. [5]

---

[3] See Marriott news release ñMarriott Announces Starwood Reservation Guest Database Security Incidentò available online at http://news.marriott.com/2018/11/marriott-announces-starwood-guest-reservation-database-security-incident

[4] *Id.*

[5] See Bloomberg article entitled ñNew York Opens Investigation Into Marriott Data Breachò, 11/30/18 available online at https://www.bloomberg.com/news/articles/2018-11-30/new-york-opens-investigation-into-marriottôs-data-breach

34. Personal and financial information is a valuable commodity. A cyber black-market exists in which criminals openly post stolen credit card numbers, Social Security numbers, and other personal information on a number of Internet websites. A credit card number trades for under $10 on the black market. Magnetic track data increases the price, and a card with full personal information such as an address, phone number, and email address (known in slang by those who hack as ñfullzò) are traded at around $25 per record.[6]

35. Marriott has admitted its shortcomings in security. Arne Sorenson, Marriottôs President and Chief Executive Officer stated, ñWe fell short of what our guests deserve and what we expect of ourselves.ò[7]

36. Marriott has begun notifying guests who were victims of the breach by email. Both Plaintiffs received such notification that they have been victimized by the breach.

37. According to *The Washington Post*, ñt][ ]he company acknowledged, however, a possible failing in the encryption security it had for credit card numbers, saying that it could not órule out the possibilityôthat encryption keys were taken by hackers, allowing access to massive troves of data. The most secure systems lock up data with encryption keys and also make sure those keys are stored safely.ò [8]

---

[6] See article entitled ñHereôs what your stolen identity goes for on the internetôs black marketò, in ñQuartzò, 7/23/15 available online at https://qz.com/460482/heres-what-your-stolen-identity-goes-for-on-the-internets-black-market/.

[7] See article ñUp to 500 million impacted by Marriott/Starwood data breachò in ñHotel News Nowò 11/30/18,m available online at http://www.hotelnewsnow.com/Articles/291666/Up-to-500m-impacted-by-Marriott-Starwood-data-breach

[8] See article entitled ñMarriott discloses massive data breach affecting up to 500 million guestsò *The Washington Post*, 11/30/18 available online at tps://www.washingtonpost.com/business/2018/11/30/marriott-discloses-massive-data-breach-impacting-million-guests/?utm_term=.398520957863

38. ñThe fact that they canôt rule out that the keys were taken sounds like a problem," said Matthew D. Green, a Johns Hopkins University cryptographer.[9]

39. Reports suggest that for most customers of Marriott, and in particular those properties that were acquired in the Starwood breach, the likeliest risk from the breach is identity theft. Such detailed personal information would make it easier for criminals to impersonate others for the purpose of conducting banking transactions, applying for government benefits or even seeking to enter secure facilities that require official identification, such as passports.

40. Government agencies and prosecutors, including the NYAG as mentioned above, in several states are investigating the data breach.

41. Furthermore, Plaintiffs and the other Class and Subclass members have suffered imminent and impending injury arising from the substantially increased risk of future fraud, identity theft and misuse posed by their PII being placed in the hands of criminals who have already, or will imminently, misuse such information.

42. Moreover, Plaintiffs have continuing interest in ensuring that their PII, which remains in the possession of Marriott, through its Starwood subsidiary, is protected and safeguarded from future breaches.

43. At all relevant times, Marriott and Starwood were well-aware, or reasonably should have been aware, that the PII collected, maintained and stored by Marriott on itsô Starwood system is highly sensitive, susceptible to attack, and could be used for wrongful purposes by third parties, such as identity theft and fraud.

44. It is well known and the subject of many media reports that PII, particularly PII that includes passport numbers, is highly coveted and a frequent target of hackers. Despite the

[9] *Id.*

frequent public announcements of data breaches, Marriott and Starwood continued to use an outdated, insufficient and inadequate system to protect the PII of Plaintiffs and the other Class and Subclass members.

45. PII is a valuable commodity because it contains not only payment card numbers but other PII as well. A cyber black market exists in which criminals openly post stolen payment card numbers and other personal information on a number of underground Internet websites. It is common knowledge that PII is considered gold to identity thieves because they can use victimsô personal data to incur charges on existing accounts, or clone ATM, debit, or credit cards.

46. At all relevant times, Marriott and Starwood knew, or in the exercise of reasonable care should have known, of the importance of safeguarding PII and of the foreseeable consequences that would occur if its data security system was breached, including, specifically, the significant costs that would be imposed on individuals as a result of a breach.

47. Marriott and Starwood were, or should have been, fully aware of the significant number of people whose PII they collected, and thus, the significant number of individuals who would be harmed by a breach of the Starwood system.

48. Unfortunately, and as alleged below, despite all of this publicly available knowledge of the continued compromises of PII in the hands of other third parties, Marriottôs and Starwoodôs approach to maintaining the privacy and security of the PII of Plaintiffs and the other Class and Subclass members, and reporting any violation thereof in accordance with law, was lackadaisical, cavalier, reckless, or at the very least, negligent.

49. The ramifications of Marriott and Starwoodôs failure to keep Plaintiffsô and other Class and Subclass membersô data secure are very significant.

50. The Federal Trade Commission (the ñFTCò) defines identity theft as ña fraud committed or attempted the identifying information of another person without authority.ò[10] The FTC describes ñidentifying informationò as ñany name or number that may be used, alone or in conjunction with any other information, to identify a specific person.ò[11]

51. Personal identifying information is a valuable commodity to identity thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, ñthey can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance.ò[12]

52. Javelin Strategy and Research reports that identity thieves have stolen $112 billion in the past six years.[13]

53. Reimbursing a consumer for a financial loss due to fraud does not make that individual whole again. On the contrary, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justiceôs Bureau of Justice Statistics (ñBJSò) found that identity theft victims ñreported spending an average of about 7 hours clearing up the issuesò and resolving the consequences of fraud in 2014.[14]

---

[10] 17 C.F.R § 248.201 (2013).

[11] *Id.*

[12] Federal Trade Commission, *Warning Signs of Identity Theft*, available at: https://www.consumer.ftc.gov/articles/0271-warning-signs-identity-theft (last visited Nov. 22, 2017).

[13] *See* https://www.javelinstrategy.com/coverage-area/2016-identity-fraud-fraud-hits-inflection-point (last visited Nov. 22, 2017).

[14] Victims of Identity Theft, 2014 (Sept. 2015) available at: http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited Nov. 22, 2017).

54. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII or PCD is stolen and when it is used. According to the U.S. Government Accountability Office (ñGAOò), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

55. Plaintiffs and the other Class and Subclass members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

56. The PII of Plaintiffs and the other Class and Subclass members is private and sensitive in nature and was left inadequately protected by Marriott.

57. The Data Breach was a direct and proximate result of Marriott and Starwoodôs failure to properly safeguard and protect Plaintiffsô and the other Class and Subclass membersô PII from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law, including Marriottôs failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiffsô and the other Class and Subclass membersô PII to protect against reasonably foreseeable threats to the security or integrity of such information.

58. Marriott and Starwood had the resources to prevent a breach, but neglected to timely and adequately invest in data security, despite the growing number of well-publicized data breaches.

---

[15] GAO, Report to Congressional Requesters, at 29 (June 2007), available at http://www.gao.gov/new.items/d07737.pdf (last visited Nov. 22, 2017).

59. Had Marriott and Starwood remedied the deficiencies in its data security systems, followed security guidelines, and adopted security measures recommended by experts in the field, they could have prevented the Data Breach and, ultimately, the theft of its customersô PII.

60. As a direct and proximate result of Marriott and Starwoodôs wrongful actions and inaction and the resulting Data Breach, Plaintiffs and the other Class and Subclass members have been placed at an imminent, immediate, and continuing increased risk of fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and effort to mitigate the actual and potential impact of the Data Breach on their lives.

61. While the PII of Plaintiffs and the other members of the Class and Subclass have been stolen, Marriott continues to hold PII of consumers, including Plaintiffs and the other Class and Subclass members. Particularly because Marriott and Starwood have demonstrated an inability to prevent a breach and immediately disclose it even after being detected, Plaintiffs and the other members of the Class and Subclass have an undeniable interest in insuring that their PII is secure, remains secure, is properly and promptly destroyed and is not subject to further theft.

## COUNT I

## NEGLIGENCE
## (ON BEHALF OF PLAINTIFFS AND THE OTHER MEMBERS OF THE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE OTHER MEMBERS OF THE SEPARATE SUBCLASS)

62. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein except to the extent any such allegations are for willful, intentional, grossly negligent or reckless misconduct.

63. Upon accepting and storing the PII of Plaintiffs and the other Class and Subclass members in its computer systems and on its networks, Defendants undertook and owed a duty to Plaintiffs and the other Class and Subclass members to exercise reasonable care to secure and

safeguard that information and to use commercially reasonable methods to do so. Defendants knew that PII was private and confidential and should be protected as private and confidential.

64. Defendants owed a duty of care not to subject Plaintiffs, and the other Class and Subclass members, to an unreasonable risk of harm because they were foreseeable and probable victims of any inadequate security practices.

65. Defendants owed numerous duties to Plaintiffs and to members of the other members of the Class and Subclass, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting and protecting PII in its possession;

b. to protect PII using reasonable and adequate security procedures and systems that are compliant with industry-standard practices; and

c. to implement processes to quickly detect a data breach and to timely act on warnings about data breaches.

66. Defendants also breached their duty to Plaintiffs and the other Class and Subclass members to adequately protect and safeguard their PII by negligently disregarding standard information security principles, despite obvious risks. Further, Defendants negligently failed to provide adequate supervision and oversight of the PII with which it was entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted an unknown third party to gather PII of Plaintiffs and the other Class and Subclass members, misuse the PII and intentionally disclose it to others without consent.

67. Defendants knew, or should have known in the exercise of reasonable care, of the risks inherent in collecting and storing PII, the vulnerabilities of its data security systems, and the

importance of adequate security. Defendants knew about numerous, well-publicized data breaches.

68. Defendants knew, or in the exercise of reasonable care, should have known, that the Starwood data systems and networks did not adequately safeguard Plaintiffsô and the other Class and Subclass membersô PII.

69. Defendants breached their duties to Plaintiffs and the other Class and Subclass members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and the other Class and Subclass members.

70. Because Defendants knew, or in the exercise of reasonable care, should have known that a breach of the Starwood data systems would damage millions of individuals, including Plaintiffs and the other Class and Subclass members, Defendants had a duty to adequately protect the Starwood data systems and the PII contained thereon.

71. Defendantsô own conduct also created a foreseeable risk of harm to Plaintiffs and the other Class and Subclass members and their PII. Defendantsô misconduct included failing to: (1) secure its systems, despite knowing their vulnerabilities, (2) comply with industry standard security practices, (3) implement adequate system and event monitoring, and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

72. Defendants also had independent duties under state and/or federal laws that required it to safeguard Plaintiffsô and the other Class and Subclass membersô PII.

73. Defendants breached their duties to Plaintiffs and the other Class and Subclass members in numerous ways, including:

a. by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard PII of Plaintiffs and the other Class and sub-Class members;

b. by creating a foreseeable risk of harm through the misconduct previously described;

c. by failing to implement adequate security systems, protocols and practices sufficient to protect Plaintiffsô and the other Class and Subclass membersô PII both before and after learning of the Data Breach; and

d. by failing to comply with the minimum industry data security standards during the period of the Data Breach.

74. Through Defendantsô acts and omissions described in this Complaint, including Defendantsô failure to provide adequate security and its failure to protect the PII of Plaintiffs and the other Class and Subclass members from being captured, accessed, disseminated, stolen and misused, Defendants unlawfully breached their duty to use reasonable care to adequately protect and secure the PII of Plaintiffs and the other Class and Subclass members during the PII was being hacked.

75. Upon information and belief, Marriott and Starwood improperly and inadequately safeguarded PII of Plaintiffs and the other Class and Subclass members in deviation of standard industry rules, regulations, and practices at the time of the unauthorized access. Defendantsô failure to take proper security measures to protect sensitive PII of Plaintiffs and the other Class and Subclass members, as described in this Complaint, created conditions conducive to a foreseeable, intentional criminal act, namely the unauthorized access of PII of Plaintiffs and the other Class and Subclass members.

76. Defendantsô conduct was negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; failing to provide adequate and appropriate supervision of persons having access to PII of Plaintiffs and the other Class and Subclass members; and failing to provide Plaintiffs and the other Class and Subclass members with timely and sufficient notice that their sensitive PII had been compromised.

77. Neither Plaintiffs nor the other Class or Subclass members contributed to the Data Breach and subsequent misuse of their PII as described in this Complaint.

78. As a direct and proximate result of the Defendantsô conduct, Plaintiffs and the other members of the Class and Subclass suffered damages including, but not limited to, loss of control of their PII, the burden and cost of heightened monitoring for signs for identity theft and for undertaking actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

## COUNT II

## NEGLIGENCE *PER SE* (ON BEHALF OF PLAINTIFFS AND THE OTHER MEMBERS OF THE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE OTHER MEMBERS OF THE SEPARATE SUBCLASS FOR VIOLATION OF SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT)

79. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein except to the extent any such allegations are for willful, intentional, grossly negligent or reckless misconduct.

80. Section 5 of the FTC Act prohibits ñunfair . . . practices in or affecting commerce,ò including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Starwood and Marriott, of failing to use reasonable measures to protect PII of

their customers. The FTC publications and orders described above also form part of the basis of Defendantsô duty in this regard.

81. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and not complying with applicable industry standards, as described in detail herein.

82. Defendantsô violation of Section 5 of the FTC Act constitutes negligence *per se*.

83. Plaintiffs and the other Class and Subclass members are within the class of persons that the FTC Act was intended to protect.

84. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the other members of the Class and Subclass.

85. As a direct and proximate result of the Defendantsô conduct, Plaintiffs and the other members of the Class and Subclass suffered damages including, but not limited to, loss of control of their PII, the burden and cost of heightened monitoring for signs for identity theft and for undertaking actions such as credit freezes and alerts to prevent identity theft, and remediating acts and damages caused by identity theft, and other economic damages.

## COUNT III

## BREACH OF IMPLIED CONTRACT (ON BEHALF OF PLAINTIFFS AND THE OTHER MEMBERS OF THE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE OTHER MEMBERS OF THE SEPARATE STATEWIDE SUBCLASS)

86. Plaintiffs incorporate and re-allege the allegations contained in the preceding paragraphs as if fully set forth herein.

87. By providing Plaintiffs and the other Class and Subclass membersô PII to Starwood and/or Marriott as customers, Plaintiffs and the other members of the Class and Subclass entered into implied contracts with Starwood and/or Marriott pursuant to which Starwood and/or Marriott agreed to safeguard and protect such information from unauthorized access and theft.

88. Plaintiffs and the other members of the Class and Subclass fully performed their obligations under the implied contracts with Marriott and/or Starwood.

89. Defendants breached the implied contracts they had made with the Plaintiffs and the other members of the Class and Subclass by failing to safeguard and protect their PII, and by allowing unauthorized access to Starwood and/or Marriottôs software application network and the mass exporting of PII from Starwood and/or Marriott.

90. The damages to Plaintiffs and the other members of the Class and Subclass as described herein were the direct and proximate result of the Defendantsô breaches of these implied contracts.

## COUNT IV

## DECLARATORY JUDGMENT (ON BEHALF OF PLAINTIFFS AND THE OTHER MEMBERS OF THE CLASS, OR, ALTERNATIVELY, PLAINTIFFS AND THE OTHER MEMBERS OF THE SEPARATE STATEWIDE SUBCLASS)

91. Plaintiffs incorporate and re-allege all allegations contained in the preceding paragraphs as if fully set forth herein.

92. As previously alleged, Plaintiffs and the other Class and Subclass members entered into an implied contract that required Marriott and/or Starwood to provide adequate security for the PII it collected from their payment card transactions. As previously alleged,

Marriott and Starwood owe duties of care to Plaintiffs and the other Class and Subclass members that require it to adequately secure PII.

93. Marriott and/or Starwood still possess PII pertaining to Plaintiffs and the other Class and Subclass members.

94. Neither Marriott nor Starwood have made announcements or notification that they have remedied the vulnerabilities in their computer data systems.

95. Accordingly, Marriott and Starwood have not satisfied their contractual obligations and legal duties to Plaintiffs and the other Class and Subclass members.

96. Actual harm has arisen in the wake of the Marriott and/or Starwoodôs Data Breach regarding Marriott and/or Starwoodôs contractual obligations and duties of care to provide data security measures to Plaintiffs and the other Class and Subclass members.

97. Plaintiffs, therefore, seeks a declaration that (a) Marriottôs and Starwoodôs existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Marriott and Starwood must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Marriottôs and Starwoodôs systems on a periodic basis, and ordering Marriott and Starwood to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting PII by, among other things, creating firewalls and access controls so that if one area of Marriott or Starwood is compromised, hackers cannot gain access to other portions of Marriott and/or Starwoodôs data systems;

e. purging, deleting, and destroying in a reasonable secure manner PII not necessary for its provisions of services;

f. conducting regular database scanning and securing checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its customers about the threats they face as a result of the loss of their financial and personal information to third parties, as well as the steps Marriott customers must take to protect themselves.

**COUNT V**

**VIOLATION OF NEW JERSEY'S CONSUMER FRAUD ACT, N.J. STAT. ANN. § 56:8-1, *ET SEQ*. (ON BEHALF OF PLAINTIFF WEINBERG AND THE OTHER MEMBERS OF THE NEW JERSEY SUBCLASS)**

98. Plaintiff Weinberg incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein.

99. The New Jersey Consumer Fraud Act prohibits the ñuse or employment by any person of any unconscionable commercial practice, deception or fraud, false pretense, false promise or misrepresentation, or the knowing concealment, suppression or omission of any material fact with the intent that others rely upon such concealment, suppression or omission, in

connection with the sale or advertisement of any merchandise or real estateé is declared to be an unlawful practiceé ò

100. Plaintiff Weinberg and the other members of the New Jersey Subclass never would have provided their sensitive and personal PII if they had been told or knew that Marriott and/or Starwood failed to maintain sufficient security to keep such PII from being hacked and taken by others, that Marriott and/or Starwood failed to maintain the information in encrypted form.

101. Marriott and/or Starwoodôs practices, acts, policies and course of conduct are actionable in that:

a. Marriott and Starwood actively and knowingly misrepresented or omitted disclosure of material information to Plaintiff and the other members of the New Jersey Subclass at the time they provided Marriot and Starwood with their PII information that did not have sufficient security or mechanisms to protect PII; and

b. Marriott and Starwood failed to give adequate warnings and notices regarding the defects and problems with its defective system of security that it maintained to protect Plaintiff and the other members of the New Jersey subclassô PII. Marriott and Starwood possessed prior knowledge of the inherent defects in its system of security and failed to give adequate and timely warnings that there had been a data breach and hacking episodes had occurred.

102. The aforementioned conduct is and was materially deceptive, false, and fraudulent and constitutes an unconscionable commercial practice in that Marriott and Starwood have, by the use of false or deceptive statements and/or knowing intentional material omissions

misrepresented and/or concealed the defective security system they maintained and failed to reveal the data breach timely and adequately.

103. Plaintiff Weinberg and the other members of the New Jersey Subclass were deceived by and relied upon Marriottôs and/or Starwoodôs misrepresentations and/or failures to disclose material facts regarding the security of their PII and the hacking of the Starwood reservation system data base.

104. Such acts by Marriott and Starwood are and were deceptive acts or practices which are and/or were, likely to mislead a reasonable consumer providing their PII to Marriott and/or Starwood. Said deceptive acts and practices aforementioned are material. The requests for and use of such PII materials in New Jersey and concerning New Jersey residents and/or citizens was a consumer-oriented and thereby falls under the New Jersey Consumer Fraud Act.

105. Marriott and Starwoodôs wrongful conduct caused Plaintiff Weinberg and the other members of the New Jersey Subclass to suffer a consumer-related injury and ascertainable losses by causing them to incur substantial expense to protect from misuse of the PII materials by third parties and placing Plaintiff Weinberg and the other members of the New Jersey Subclass at serious risk for incurring monetary damages.

106. In addition to or in lieu of actual damages, because of the injury, Plaintiff Weinberg and the other members of the New Jersey Subclass seek treble damages, attorneysô fees and costs for each injury and violation which has occurred.

## COUNT VI

### VIOLATION OF FLORIDA'S DECEPTIVE AND UNFAIR TRADE PRACTICES ACT, Fla. Stat. §§ 501.201, *et seq*.
### (ON BEHALF OF PLAINTIFF NEIKIRK AND THE OTHER MEMBERS OF THE FLORIDA SUBCLASS)

107. Plaintiff Neikirk (ñPlaintiffs,ò for purposes of this Count), individually and on behalf of the other Florida Subclass members, repeats and re-alleges the allegations hereinabove as though fully set forth herein.

108. At all relevant times, Plaintiff and Florida Subclass members were ñconsumersò within the meaning of the Florida Deceptive and Unfair Trade Practices Act, Fla. Stat § 501.201 *et seq.* (ñFDUTPAò).

109. Defendants are engaged in trade and commerce in Florida.

110. Plaintiff and the Florida Subclass entrusted Defendants with their PII.

111. As alleged in this Complaint, Marriott and Starwoods engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including the following, in violation of the FDUTPA:

a. failure to maintain the security of credit and/or debit card account information;

b. failure to maintain adequate computer systems and data security practices to safeguard credit and debit card information and other PII;

c. failure to disclose that its security systems and data security practices were inadequate to safeguard personal and private information and other PI from theft;

d. continued acceptance of PII and storage of other Private Information after Defendants knew or should have known of the security vulnerabilities of the systems that were exploited in the Security Breach; and

e. allowing unauthorized persons to have access to Defendantsô customersô accounts.

112. Defendants knew or should have known that its security systems and data security practices were inadequate to safeguard the PII of Plaintiff and Florida Subclass members, deter

hackers, and detect a breach within a reasonable time, and that the risk of a data breach was highly likely.

113. As a direct and proximate result of Defendantsô violation of FDUTPA, Plaintiff and the Florida Subclass suffered damages including, but not limited to:

a. theft of their personal and financial information;

b. improper disclosure of their PII;

c. the imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PII being placed in the hands of criminals and potential sale of Plaintiffsô and Class membersô information on the Internet black market; and

d. damages to and diminution in value of their PII entrusted to Defendants and the loss of Plaintiffsô and Class membersô privacy.

114. As a direct result of Defendantsô knowing violation of FDUTPA, Plaintiffs and the Florida Subclass are entitled to damages as well as injunctive relief, including, but not limited to:

a. ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendantsô systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;

b. ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;

c. ordering that Defendants segment PII by, among other things, creating firewalls and access controls so that if one area of the Company is compromised, hackers cannot gain access to other portions of the Companyôs systems;

d. ordering that the Company purge, delete, and destroy in a reasonably secure manner PII not necessary for its provisions of services;
e. ordering that Defendants conduct regular database scanning and security checks;
f. ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and
g. ordering Defendants to meaningfully educate their users about the threats they face as a result of the loss of their financial and Private Information to third parties, as well as the steps its customers must take to protect themselves.

115. Plaintiffs brings this action on behalf of herself and Florida Subclass members for the relief requested above and for the public benefit in order to promote the public interests in the provision of truthful, fair information to allow consumers to make informed purchasing decisions and to protect Plaintiffs and Florida Subclass members and the public from Marriott and Starwoodôs unfair methods of competition and unfair, deceptive, fraudulent, unconscionable and unlawful practices. Defendantsô wrongful conduct as alleged in this Complaint has had widespread impact on the public at large.

116. Plaintiffs and the Florida Subclass seek actual damages under Fla. Stat. § 501.211(2) and all fees, costs, and expenses allowed by law, including attorneyôs fees and costs, pursuant to Federal Rule of Civil Procedure 23 and Fla. Stat. §§ 501.2105 and 501.211, to be proven at trial.

## COUNT VII

### VIOLATION OF THE NEW JERSEY DATA BREACH ACT (ON BEHALF OF PLAINTIFFS WEINBERG AND THE OTHER MEMBERS OF THE NEW JERSEY SUBCLASS)

117. Plaintiffs Weinberg incorporates and re-alleges all allegations contained in the preceding paragraphs as if fully set forth herein except to the extent any such allegations are for willful, intentional, grossly negligent or reckless misconduct.

118. Plaintiffs Weinberg and the other members of the New Jersey subclass are consumers who provided PII to Marriott and Starwood for personal and private use.

119. By failing to timely notify Marriott and/or Starwood customers of the Data Breach, Marriott violated N.J. Stat. Ann. §56:8-163(a), et seq., which provides:

> a. Any business that conducts business in New Jersey, or any public entity that compiles or maintains computerized records that include personal information, shall disclose any breach of security of those computerized records following discovery or notification of the breach to any customer who is a resident of New Jersey whose personal information was, or is reasonably believed to have been, accessed by an unauthorized person. The disclosure to a customer shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subsection c. of this section, or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system. Disclosure of a breach of security to a customer shall not be required under this section if the business or public entity establishes that misuse of the information is not reasonably possible. Any determination shall be documented in writing and retained for five years.
>
> * * *
>
> (c)(2) The notification required by this section shall be delayed if a law enforcement agency determines that the notification will impede a criminal or civil investigation and that agency has made a request that the notification be delayed. The notification required by this section shall be made after the law enforcement agency determines that its disclosure will not compromise the investigation and notifies that business or public entity.
>
> * * *
>
> 56:8-166 It shall be an unlawful practice and a violation of P.L. 1960, c.39 (C.56:8-1 et seq.) to willfully, knowingly or recklessly violate sections 10 through 13 of this amendatory and supplementary act.

120. The Marriott Data Breach constituted a breach of the Marriott security system within the meaning of the above New Jersey data breach statute and the data breached was protected and covered by the data breach statute.

121. Marriott unreasonably delayed informing the public, including Plaintiffs Weinberg and the other members of the New Jersey Subclass, about the Data Breach after Marriott and/or Starwood knew or should have known that the Data Breach had occurred.

122. While the Data Breach and stealing of customerôs personal information was known or should have been known to Marriott and/or Starwood, neither Marriott or Starwood made a public announcement of the Data Breach until November 30, 2018, and at that time still had not provided direct information of a hacking to its customers. By the Companyôs admission the Data Breach began as early as 2014 and Marriott and/or Starwood knew or should have known of the Data Breach long before November 30, 2018. Moreover, by September 10, 2018, Marriott was almost fully aware of the Data Breach, yet failed to notify its customers.

123. Thus, Marriott and/or Starwood failed to disclose the Data Breach to Plaintiffs Weinberg and the other members of the New Jersey subclass without unreasonable delay and in the most expedient time possible.

124. Marriott and/or Starwood provided no indication that any law enforcement agency requested that Marriott delay notification. Plaintiffs Weinberg and the other members of the New Jersey subclass suffered harm directly resulting from Marriott and/or Starwoodôs failure to provide and the delay in providing notification of the data breach with timely and accurate notice as required by law.

125. As a result of said practices, Marriott and/or Starwood have directly, foreseeably, and proximately caused damages to Plaintiffs and the other members of the New Jersey subclass.

Had Marriott and/or Starwood provided timely and accurate notice of the Data Breach Plaintiffs and the other members of the subclass would have been able to avoid and/or attempt to ameliorate or mitigate the damages and harm resulting in the unreasonable delay by Marriott and Starwood in providing notice. Plaintiffs and the New Jersey subclass members could have avoided providing further data to Marriott and/or Starwood could have avoided use of Marriott and/or Starwoodôs services, and otherwise have tried to avoid the harm caused by Marriottôs delay in providing timely and accurate notice.

**COUNT VIII**

**VIOLATION OF MARYLAND CONSUMER PROTECTION ACT,**
**Maryland Code, Commercial Law Article § 13-101, et seq.**
**(Brought on Behalf of Plaintiffs and the other members of the Class (Nationwide))**

126. Plaintiffs repeat and reaffirm the assertions of fact contained in the forgoing paragraphs as though fully set forth herein.

127. Among other things, Marylandôs Consumer Protection Act (ñMCPAò) prohibits ñunfair or deceptive trade practicesò in a variety of circumstances, including the ñsale ... of consumer good é or consumer services.ò CL §13-303(1).

128. The statute lists various ways of committing unfair or deceptive trade practices. For example, a violation may involve an affirmative ñfalse ... or misleading oral or written statement ... or other representation of any kind which has the capacity, tendency, or effect of deceiving or misleading consumers.ò CL §13-301(1).

129. Prohibited representations include representations that ñConsumer goods, é or consumer services have a sponsorship, approval, accessory, characteristic, ingredient, use, benefit, or quantity which they do not have,ò CL §13-301(2)(i), and ñConsumer goods, consumer

realty, or consumer services are of a particular standard, quality, grade, style, or model which they are not,ò CL §13.301(2)(iv).

130. A violation may also consist of an omission ð i.e., a ñfailure to state a material fact if the failure deceives or tends to deceive.ò CL §13-301(3). It is not necessary that a consumer actually have been misled or damaged as a result of the practice. CL §13-302.

131. The Act also prohibits ñDeception, fraud, false pretense, false premise, misrepresentation, or knowing concealment, suppression, or omission of any material fact with the intent that the consumer rely on the same in connection with é (i) the promotion or sale of any consumer goodsé .ò *Id.* at 13

132. The Act is to be construed liberally to promote the protection of consumers. CL §§13-105, 13- 102(3).

133. The Act includes an explicit private cause of action since 1973. Chapter 73, Laws of Maryland 1973, codified at CL §13-408. In particular, ñany person may bring an action to recover for injury or loss sustained by him as the result of a practice prohibited by [the Consumer Protection Act].ò CL §13-408(a).

134. Defendantsô business acts and practices alleged herein constitute unfair or deceptive trade practices under the MCPA.

135. Defendants knew of or should have known of vulnerabilities and defects in its data security systems storing PII of Plaintiffs and the other Class members before the Breach, but concealed that information in violation of the MCPA.

136. Defendants violated the MCPA by failing to disclose and actively concealing known data-security defects, and by otherwise deceiving Plaintiffs and the Class members.

137. More specifically, Defendants engaged in unfair or deceptive trade practices by misrepresenting or omitting material facts to Plaintiffs and the other Class members regarding the adequacy of its data security procedures protecting PII; misrepresenting or omitting material facts to Plaintiffs and the other Class members regarding its failure to comply with relevant state and federal laws designed to protect consumersô privacy and PII; and failing to discover and disclose the data breach to Plaintiffs and the other members of the Class in a timely and accurate manner.

138. These deceptive acts and practices were likely to and did deceive Plaintiffs and the other Class members regarding the lack of security protecting their PII.

139. Defendants intentionally and knowingly misrepresented such material facts with an intent to mislead Plaintiffs and the other Class members.

140. Defendants owed Plaintiffs and the other Class members a duty to disclose its data-security defects because Defendants possessed exclusive knowledge regarding the vulnerability of the PII, concealed the data security defects from Plaintiffs and the Class members, and made incomplete representations regarding its data security systems while withholding material facts from Plaintiffs and the other Class members.

141. These representations and omissions were material to the Plaintiffs and the other Class members due to the value and sensitivity of the PII.

142. Plaintiffs and the other Class members suffered ascertainable loss as a result of Defendantsô material misrepresentations, concealment, and omissions of material information as alleged herein.

143. As a direct and proximate result of Defendantsô violation of MCPA, Plaintiffs and the other Class members have suffered damages.

144. Plaintiffs seek an order enjoining Defendantsô unfair or deceptive trade practices, and awarding attorneysô fees, and any other just and proper relief available under MCPA. Upon information and belief, Defendantsô security practices were designed, established, and initiated, at least in part from Maryland. Accordingly, Maryland has significant contacts to the claims asserted by this class so that application of its consumer fraud laws to all class claimants is not arbitrary, capricious, or unfair and is not a violation of due process.

## REQUEST FOR RELIEF

**WHEREFORE**, Plaintiffs, on behalf of themselves and all others similarly situated, respectfully requests that this Court:

A. Certify this action as a class action pursuant to Federal Rule of Civil Procedure 23(a) and (b)(3), and appoint the Plaintiffs as Class and Subclass representatives and their counsel as Class counsel;

B. Award Plaintiffs and the other members of the Class and Subclass appropriate relief, including actual and statutory damages;

C. Enter judgment in favor of Plaintiffs and the other members of the Class and Subclass and against the Defendants under the legal theories alleged herein;

D. Award reasonable attorneysô fees, costs, and expenses;

E. Award the Plaintiffs and the other members of the Class and Subclass pre-judgment and post-judgment interest at the maximum rate allowable by law;

F. Award Plaintiffs and the other members of the Class and Subclass equitable, injunctive and declaratory relief as may be appropriate under applicable laws. Plaintiffs on behalf of the other members of the Class and Subclass seeks appropriate injunctive relief designed to ensure against the recurrence of a data breach by adopting and implementing reasonable data security

practices to safeguard Plaintiffsô and class and sub-class memberôs PII, by an Order requiring Marriott and Starwood to implement reasonable data security enhancements as they become available, including data encryption, segregation of sensitive data, more robust passwords, authentication of users, increased control of access to sensitive information on the network, prohibitions of mass exports of sensitive data;

G. Enter Declaratory Judgment that seeks a declaration that (a) Marriottôs existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, Marriott must implement and maintain reasonable security measures;

H. Enter such additional orders or judgment as may be necessary to prevent a recurrence of the Data Breach and to restore any interest or any money or property which may have been acquired by means of violations set forth in this Complaint; and

I. Grant such other and further relief as the Court deems just and proper.

**JURY DEMAND**

Plaintiffs demand a trial by jury on all issues so triable.

Dated: December 24, 2018

Respectfully submitted,

Nicholas A. Migliaccio, Esq.
(Maryland Federal Bar No. 29077)
Jason S. Rathod
(Maryland Federal Bar No. 18424)
**MIGLIACCIO & RATHOD LLP**
412 H Street NE, Ste. 302

Washington, DC 20002
Tel: (202) 470-3520
nmigliaccio@classlawdc.com
jrathod@classlawdc.com

Gary S. Graifman *
Jay Brody *
**KANTROWITZ GOLDHAMER & GRAIFMAN, P.C.**
747 Chestnut Ridge Rd.
Chestnut Ridge, NY 10977
Tel: (845) 356-2570
Fax: (845) 356-4335
ggraifman@kgglaw.com
jbrody@kgglaw.com

* *pro hac vice* admission to be sought

Attorneys for the Plaintiffs and Putative Class